WEST Search History

Hide Items | Restore | Clear | Cancel

DATE: Wednesday, February 25, 2004

Hide?	Set Name	Query	Hit Count
		DB=USPT; PLUR=YES; OP=ADJ	
□	L12	6035104.pn.	1
□	L11	L10 and header	14
□	L10	L9 and (email or e mail or e-mail or electronic mail)	23
□	L9	l5 and client and server	80
□	L8	l5 and client ann server	0
□	L7	L5 same email	0
□	L6	L5 same email	0
□	L5	check$ same memory same capacity	1933
□	L4	email and L2	1
□	L3	email and L2	1
□	L2	L1 and client and server	4
□	L1	blackberry	1031

END OF SEARCH HISTORY

First Hit Fwd Refs

End of Result Set

□ Generate Collection Print

L14: Entry 1 of 1 File: USPT Dec 4, 2001

DOCUMENT-IDENTIFIER: US 6327656 B1

**** See image for Certificate of Correction ****

TITLE: Apparatus and method for electronic document certification and verification

Brief Summary Text (11):

According to one aspect of the present invention, a party with an electronic document can make a request for electronic document certification. The certification can, for example, be provided by an Internet server. The certification provider receives the party's request for certification, along with the electronic document to be certified. To perform certification, a unique digital signature is extracted from the electronic document. The extracted signature provides a document "fingerprint" that serves to identify the document and to distinguish the document from other documents, even ones that appear to be similar to one another. The certification provider also stores and maintains certification information including the unique digital signature for the document in association with an identification code. The certification information can also include additional information, such as an indication of the exact time and date of certification. The identification code (and optionally a copy of the certified document) can be provided to the party making the request for certification, or to any relevant party.

Drawing Description Text (3):

FIG. 1 is a schematic illustrating exemplary interconnections between a client and a wide area network server in accordance with the present invention.

Detailed Description Text (2):

Referring now to the schematic diagram of FIG. 1, the electronic document certification application and method of certification of the present invention preferably operate on a system wherein a client-server relationship can be established between a certification provider 200 (the server) and any one of a plurality of clients 100. The certification provider 200 is a server that includes the apparatus and uses the method of electronic document certification and verification in accordance with the present invention. In the system illustrated in FIG. 1, the certification provider 200 resides on a wide area network (WAN) such as the network typically referred to as the Internet or World Wide Web. Various exemplary interconnections are shown between clients 100 and the certification provider 200.

Detailed Description Text (3):

One way that the client-server relationship is established is shown in connection with client 100a. That client 100a is coupled to the WAN via a line 10 such as a telephone line. In this example, particularly where the WAN is the Internet, access can be provided by an Internet access provider or an Internet service provider and the client 100a includes a modem coupled to a telephone line to link to the service or access provider. Another way that the client-server relationship is established is shown in connection with client 100b. That client 100b is part of a local area network (LAN) and communication between the client 100b and the certification provider 200 can be facilitated by a connection 20 established through a LAN server

150. Although access can also be through an access or service provider, the connection 20 can be by other conventional means such as a leased line.

Detailed Description Text (4):
Although the preferred embodiment of the present invention contemplates that the certification provider 200 is an Internet server, the ordinarily skilled artisan will recognize the various alternatives for establishing a client-server connection between the certification provider 200 and a client 100, such as interconnection within a local area network of computers or over any internetwork connection of computers. Additionally, although the electronic document certification application is shown to reside at a server, it is understood that any computer can be used, and that access to the application can be provided in ways other than through the preferred client-server arrangement. For example, a document on a floppy disk can be certified by inserting the floppy disk into the relevant port of a personal computer including the electronic document certification application, which could return relevant certification information to the floppy disk. In such an instance, the certification provider can reside at the personal computer, and the client server relationship is not required The artisan will recognize the various alternatives for providing certification according to the principles of the present invention.

Detailed Description Text (5):
Preferably, the certification provider 200 uses a UNIX operating system, although any conventional operating system such as Windows NT could be used. The certification provider 200 also implements conventional internet communication protocols such as the transmission control protocol/internet protocol (TCP/IP) suite. Additionally, although a preferred embodiment uses the conventional simple mail transfer protocol (SMTP), the certification provider 200, in conjunction with the use of the electronic document certification application, can implement other communication protocols such as the file transfer protocol (FTP) and/or the Hypertext Transfer Protocol (HTTP) for the transfer of files or other information between the client 100 and the provider 200. Additionally, although functions for certification and verification can be provided at the certification provider 200, functions can also be undertaken by providing executable code to the client 100 (such as by implementing Java applets or ActiveX objects that are transmitted from server to client).

Detailed Description Text (6):
Although a more detailed embodiment of electronic document certification and verification is described with reference to the block diagram of FIG. 2B and flow charts of FIGS. 3-5 below, the interaction between the client 100 and certification provider (server) 200 are basically as follows. After communication between the certification provider 200 and a client 100 are established according to network protocols, the certification provider 200 operates to receive a request, from a user at the client 100 side, to certify an electronic document. The document will typically be included in the request.

Detailed Description Text (9):
Provision of the identification code to the certification requester allows subsequent verification as follows. Assume that a client 100 user later wants to verify that a document in question was previously certified. The client 100 would request verification and provide, again using network signal transmission protocols, the identification code and the document in question to the certification provider 200. The certification provider 200 receives the request for verification, and first determines the identification code. The certification provider 200 then determines whether the identification code exists in its maintained certification information, and, if so, locates the digital signature that is associated with the code. Then, preferably using the same process used for certification, the certification provider 200 extracts a digital signature from the document to be verified. If the newly extracted digital signature matches the

digital signature from certification, a positive verification that the document is the one that had been certified is established. The positive verification result is transmitted to the verification requester.

Detailed Description Text (10):
Referring now to the block diagram of FIG. 2A, an embodiment of a WAN certification provider 200 including an electronic document certification application is illustrated. The certification provider 200 comprises a central processing unit (CPU) 212, memory 214, data storage device 216, I/O ports 218, a network link 220, and a clock 222. The CPU 212 is a conventional processor such as a Pentium Pro as provided by Intel Corporation, Santa Clara, Calif., the data storage device 216 is a conventional storage device such as a hard disk, the I/O ports 218 provide conventional local data input and output. A bus 210 couples the CPU 212, memory 214, data storage device 216, I/O 218 and network line 220 in conventional fashion. The network link 220 is a conventional network interface to a network transmission line 230, and provides data to and from the server 230.

Detailed Description Text (11):
Preferably, the memory 214 includes a UNIX operating system, and is configured to transmit and receive information using the Simple Mail Transfer Protocol (SMTP). It is understood that other operating systems and other communication protocols, such as FTP and HTTP, can also be provided. The memory 214 is also configured to include the electronic document certification application. The CPU 212, at the direction of instructions provided in memory 214 so configured, and in conjunction with the various server modules 214, 216, 218, 220, and 222 operates to receive requests for electronic document certification; determine whether requests are properly registered; extract digital signatures from electronic documents; maintain certification information including extracted signatures and identification codes corresponding to them; and transmit certification information, such as identification codes, to parties pursuant to a certification requester. Similarly, verification of prior alleged certification is provided by receiving identification codes, extracting verification signatures from tested documents, and comparing digital signatures from certification to the verification signatures to determine whether they match.

Detailed Description Text (14):
A party may request certification (a "certification requester") using their computer (such as client 100) or other electronic device that can then transmit the document over the Internet or other communication medium. Certification can be requested for electronic documents that include, among other things, text, graphics, sound, music, sketches, and video clips. The document may also be encrypted, if the certification requester wishes to keep its contents protected.

Detailed Description Text (18):
It is understood that registration is optional, but if registration is used, once registration is confirmed, the document to be certified can be located (step 308) for processing by the certification module 258. In this embodiment, the contents of an electronic mail message are treated as the document to be certified. Any portions of the message that will not be certified, if any, can be removed. Thus, the certification module 258 strips the local mail headers from the message, leaving only the original headers and the contents of the message, as well as the source and destination. The date of message transmittal (such as is provided by an electronic mail sender's electronic mail program) can be ignored, as it is not typically reliable and since the certification provider 200 can implement more accurate time and date information.

Detailed Description Text (36):
Again, the certification data module 256 can provide a standard database file with entries. Preferably, the database is named according to the date, so each day a new database is used for this purpose. This keeps the size of the database files small

and easy to handle. After a database is used, it can be stored local to the certification provider 200 (such as in a local hard disk or other data storage device 216) or remotely. Additionally, the certification module 258 can use the local data storage device 216 or any storage during the certification process (i.e. the database does not have to completely reside in memory). The database could be just one file with many entries, and it could be shared by many machines, if multiple servers 200 are certifying documents (sharing the load).

Detailed Description Text (37):
The certification module then prepares (step 314) a message that can be transmitted (step 316) to the certification requester. In this embodiment, the identification code (e.g., the serial number) can be placed in a new electronic mail message (which can be referred to as the timestamp certificate) addressed to a relevant party such as the certification requester. The exact time of certification is also noted for the sender's use. The original contents of the document will be appended to the new message, with a warning to the user to keep the new message for future use, and not to make any modification.

Detailed Description Text (70):
The above example construes an entire message that is transmitted by electronic mail as the "document." Thus, the digital signature (maintained at the certification provider 200) is extracted from the entire message (less some header stripping). Additionally, it includes the entire message in the timestamp certificate. This can be advantageous because it allows a concise record of the certified document, and the identification code (here the serial number) is less likely to get lost. With this embodiment, if a standard electronic mail message with an identical text in the body of the message were sent for certification at two different times, and the time was included in the message, different signatures would be generated for each of the two certification requests.

Detailed Description Text (74):
Referring now to the flow chart of FIG. 5 along with FIG. 2B, in a first step 505, a request for certified electronic mail transmission from a sender (the certification requester) to a recipient is received by the certification provider 200. In this instance, the message to be sent by certified electronic mail is received by the certification provider 200, possibly to an alternative address (i.e., other than the "certify" address). Alternatively, the message could be sent to the "certify" address, but would include information about the recipient within the body of the message addressed to certify. Either alternative allows the certification module 258 to obtain the message recipient information. Preferably, the message would include, in the text portion, a recognizable string indicating the recipient. For example, the message could include the note "CERTIFIED ELECTRONIC MAIL, RECIPIENT=name@service.com." The message is received and scanned by the certification module 258 using conventional text parsing techniques to determine whether the message is a piece of certified electronic mail, and then to locate and isolate the recipient information. Preferably, the module 258 includes routines for providing a lexical stream scan for the capitalized portion of the above note (CERTIFIED ELECTRONIC MAIL, RECIPIENT=). Once the capitalized portion of the note is recognized within the message, the module 258 can use conventional routines to locate the recipient information (typically following the identifying note). The application 250 then certifies (in step 515) the document portion of the message (e.g., the message itself could be the document, or an attachment could be the document) as described for certification above (i.e., certification module 258 locates and obtains document; signature generation module 254 extracts digital certification signature; certification data module 256 stores certification information including time and date, digital certification signature, and serial number). Two electronic mail messages are then sent (steps 520, 525), one to the recipient of the electronic mail message, and one to the sender. The recipient receives the message with a warning indicating that the message had been sent by certified electronic mail. The sender would receive a message similar to the

described timestamp certificate. That message could indicate that the mail certification process was successful, that the transmission was delivered to recipient (e.g., name@service.com), and could include a copy of the original message and an associated serial number for subsequent verification procedures.

Detailed Description Text (80):
The verification module 260 includes routines for segregating the document to be verified from the serial number. In this embodiment, timestamp certification is sent to a "verify" address as an electronic mail message (e.g., "verify@timestamp.com"). After stripping away superfluous header information as in the certification process, the serial number is located from within the message (step 410). This is done using conventional techniques, for example by scanning the message for the introductory language ("Timestamp Serial Number:") and then obtaining the serial number that is associated with it.

Detailed Description Text (85):
Conventional programming techniques, such as those incorporating a scan for the above string for the header and footer, are used to locate the subject document. First, the message is scanned for the header (the string including "DOCUMENT START", after the header is found, the text following it is loaded into a buffer in memory, until the footer is found (the string including "DOCUMENT END"). If necessary, any footer can be removed from the buffer. The verification module 260 accesses the document and operates in conjunction with the signature generation module 254 to apply the same signature extraction process that was provided at certification to the document (step 416). Where different signature extraction processes are provided, the module 254 can be appropriately configured according to the maintained information about the particular process.

Detailed Description Text (108):
Although the present invention has been described with reference to certain preferred embodiments, those skilled in the art will recognize that various modifications may be provided. For example; although separate modules for registration, signature generation, verification and certification are described, it is understood that the various processes may be integrated into common modules or subdivided into additional modules which perform equivalent functions. Additionally, although electronic mail is described in an embodiment, it is understood that other network protocols could be used to transmit information to and from the certification server for both certification and verification. Additionally, direct provision of documents, such as through a floppy disk, can also be provided. These and other variations upon and modifications to the described embodiments are provided for by the present invention which is limited only by the following claims.

CLAIMS:

14. A computer system for processing certification requests, verification requests and forwarding requests for electronic documents, the computer system comprising:

a central processing unit for making registration determinations, certification determinations, verification determinations and forwarding determinations;

a communication module to establish a network connection and receiving data from clients, the communication module communicatively coupled to the central processing unit for communicating with the clients;

a certification module for processing the certification requests, the certification module communicatively coupled to the central processing unit for receiving signals in response to the central processing unit making the certification determinations, and the certification module further communicatively coupled to the communication module for communicating with the clients;

a verification module for processing the verification requests, the verification module communicatively coupled to the central processing unit for receiving signals in response to the central processing unit making the verification determinations, and the verification module further communicatively coupled to the communication module for communicating with the clients;

a signature generation module to generate unique signatures for the electronic documents, the signature generation module communicatively coupled to the certification module to provide the unique signatures for the electronic documents in response to the communication module receiving the certification requests; and

a certification data module to maintain database records for permanently storing information about the electronic documents, the information including the unique signatures for the electronic documents, and receiving time and date of the requests, the certification data module communicatively coupled to the certification module for receiving the unique signatures for the electronic documents, further communicatively coupled to the central processing unit for obtaining the time and date of the certification requests and the forwarding requests, and the certification data module further communicatively coupled to the verification module for providing the information about the electronic documents in response to the verification requests.

15. The apparatus of claim 14, further comprising:

a registration module for generating and verifying clients' registration information, the registration module communicatively coupled to the central processing unit, the central processing unit signaling the certification module upon making the registration determinations, and the registration module further communicatively coupled to the communication module for communicating with the clients.

16. The apparatus of claim 14, wherein the certification module further includes routines for receiving an electronic mail message at a certification address; scanning the electronic mail message to locate a recipient address; sending the electronic mail message with the electronic document to the recipient address; and sending a confirmation message including the certification identifier to the clients.